AMENDMENTS TO THE SPECIFICATION

1. Page 2, third paragraph (starting at line 14 and continuing to page 3 line 2), delete the entire paragraph and replace with:

Block ciphers such as the Data Encryption Standard (DES) are popularly used for encryption of computer communications. However, empirical evidence indicates that stream ciphers are faster than block ciphers at equivalent security levels. For example, in practical evaluation, the stream ciphers RC4 and SEAL have been d4etermined to be significantly faster than any secure block cipher when implemented on general-purpose computer processors. Further, ~~and~~ RC4 and SEAL have survived years of scrutiny by cryptanalysts. SEAL is described in U.S. Pat. No. 5,454,039; U.S. Pat. No.5,675,652; U.S. Pat. No. 5,835,597; Rogaway, P. and Coppersmith, D., "A Software-Optimized Encryption Algorithm", Proceedings of the 1994 Fast Software Encryption Workshop, Lecture Notes in Computer Science, Volume 809, Springer-Verlag, 1994, pp. 56-63; Rogaway, P. and Copphersmith, D., "A Software-Optimized Encryption Algorithm", Journal of Cryptology, Volume 11, Number 4, Springer-Verlag, 1998, Pages 273-287, and at ~~http://www.cs.ucdavis.edu/~rogaway/ papers/~~ the document seal-abstract.html in the directory /~rogaway/papers/ of the "www.cs" subdomain of the Internet domain ucdavis.edu. Both SEAL and RC4 are discussed in Schneier.

2. Page 12, delete the last paragraph consisting of lines 20-26, and replace with:

The definitions of functions *f, g, d,* and *c* are

$$f(z \mid y \mid x) = 2z \mid S(R(S(R(y)))) \mid L(S(L(S(x))))$$

$$g(z \mid y \mid x) = 2z+1 \mid L(S(L(S(y)))) \mid S(R(S(R(\neg x)))))$$

$$d(z \mid y \mid x) = z \mid x + y + z \mid 2x + y + z$$

$$c(z \mid y \mid x) = x \oplus y$$

where integer addition modulo two is denoted as +, bitwise exclusive-or is denoted as $\oplus$, and bitwise complementation is denoted as $\neg$;